IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF OKLAHOMA

LANDON JOHNSON AND CLARISSA COFFEY, individually and on behalf of all similarly situated persons, Plaintiffs, v. O.K. FOODS, INC. Defendant.	Case No. CIV-21-561-J **FIRST AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs, Landon Johnson ("Mr. Johnson" or "Plaintiff Johnson") and Clarissa Coffey ("Ms. Coffey" or "Plaintiff Coffey"), individually, and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to them and upon information and belief as to all other matters, and by and through undersigned counsel, hereby bring this First Amended Class Action Complaint against Defendant, O.K. Foods, Inc. ("OK Foods"), and allege as follows:

INTRODUCTION

1. Part of the bargain of obtaining a job requires turning over to employers valuable personally identifiable information ("PII"),[1] including names, Social Security

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account

numbers, birthdates and addresses. Identity thieves can use this highly sensitive information to fraudulently open new accounts, access existing accounts, perpetrate identity fraud or impersonate victims in a myriad of schemes, all of which can cause grievous financial harm, negatively impact the victim's credit scores for years, and cause victims to spend countless hours mitigating the impact.

2. Every year millions of Americans have their most valuable PII stolen and sold online because of data breaches. Despite the dire warnings about the severe impact of data breaches on Americans of all economic strata, companies still fail to put adequate security measures in place to protect their customers' and employees' data.

3. OK Foods, one of the world's largest fully integrated chicken producers, is among those companies which have failed to meet their obligation to protect the sensitive PII entrusted to them by their current and former employees.

4. As reported by OK Foods, between April 22, 2020 and April 30, 2020, an unknown third party gained unauthorized access to an OK Foods employee email address that contained certain highly sensitive and unencrypted employee data. Employee names and Social Security numbers were among the PII accessed and obtained by the unauthorized party.

5. Defendant OK Foods required its employees to provide it with their sensitive PII and failed to protect it. Defendant had an obligation to secure its employees' PII by implementing reasonable and appropriate data security safeguards. This was part of the

---

number).

bargain between Plaintiffs and Class Members[2] and OK Foods.

6. As a result of OK Foods' failure to provide reasonable and adequate data security, Plaintiffs' and the Class Members' unencrypted, non-redacted PII has been exposed to unauthorized third parties. Plaintiffs and the Class are now at much higher risk of identity theft and cybercrimes of all kinds, especially considering the highly sensitive PII stolen here. This risk constitutes a concrete injury suffered by Plaintiffs and the Class, as they no longer have control over their PII, which PII is now in the hands of third-party cybercriminals. This substantial and imminent risk of identity theft has been recognized by numerous courts as a concrete injury sufficient to establish standing.[3] Furthermore, Plaintiffs and the Class, as also set forth below, will have to incur costs to pay a third-party

[2] As used herein, the terms "Class" or "Class Members" means the putative "Nationwide Class" and "Oklahoma Subclass" defined below.

[3] *See, e.g., Resnick v. AvMed, Inc*., 693 F.3d 1317, 1324 (11th Cir. 2012) (holding that the misuse of plaintiff's sensitive information to open a bank account was sufficient to confer standing even where she did not allege any "unreimbursed losses"); *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388 (6th Cir. 2016) (finding injury-in-fact for data breach case and defining "actual misuse" as a "fraudulent charge"); *Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc.*, 892 F.3d 613, 622 (4th Cir. 2018) (standing conferred based on alleged fraudulent use of identifying information, without alleged unreimbursed expenses, because "the Supreme Court long ago made clear that 'in interpreting injury in fact ... standing [is] not confined to those who [can] show economic harm.'"); *In re Equifax, Inc. Customer Data Security Breach Litigation*, No. 20-10249, 2021 WL 2250845, at *6 (11th Cir. June 3, 2021) (holding that the plaintiffs plausibly alleged injury in fact and established standing "given the colossal amount of sensitive data stolen, including Social Security numbers, names, and dates of birth, and the unequivocal damage that can be done with this type of data…"); *McMorris v. Carlos Lopez & Associates, LLC*, 995 F.3d 295 (2d Cir. 2021) (recognizing that plaintiffs may establish Article III standing based on an increased risk of identity theft or fraud following the unauthorized disclosure of their data); *Attias v. Carefirst, Inc.*, 865 F.3d 620, 628-29 (D.C. Cir. 2017) ("The principal question, then, is whether the plaintiffs have plausibly alleged a risk of future injury that is substantial enough to create Article III standing. We conclude that they have.").

credit and identity theft monitoring service for the rest of their lives as a direct result of the Data Breach.

THE PARTIES

7. Defendant O.K. Foods, Inc., is an Arkansas corporation with numerous hatcheries, farms, feed mills, and processing plants across the country, including in Oklahoma City, Oklahoma. Its corporate headquarters are located in Fort Smith, Arkansas.

8. OK Foods is wholly owned by Bachoco USA, LLC, a Delaware corporation. Bachaco USA, LLC is a wholly owned subsidiary of Industrias Bachoco S.A. de C.V., a publicly held corporation headquartered in Guanajuato, Mexico.

9. OK Foods has evolved from a livestock and poultry feed manufacturer to one of the world's largest fully integrated chicken producers, with over three thousand five hundred (3,500) employees providing chicken products to people around the globe.

10. Plaintiff Johnson is a resident of Sequoyah County, Oklahoma and was employed by OK Foods in Muldrow, Oklahoma in or around September 2016.

11. Plaintiff Coffey is a resident of Scott County, Arkansas and was employed by OK Foods in Fort Smith, Arkansas in or around April 2016.

12. Mr. Johnson and Ms. Coffey reasonably believed OK Foods would keep their PII secure. Had OK Foods disclosed to them that their PII would not be kept secure and would be easily accessible to criminal hackers and third parties, they would have demanded OK Foods take additional precautions relating to their PII.

JURISDICTION AND VENUE

13. Subject matter jurisdiction in this civil action is authorized pursuant to 28

U.S.C. § 1332(d) because there are more than 100 Class Members, at least one class member is a citizen of a state different from that of Defendant, and the amount in controversy exceeds $5 million, exclusive of interest and costs.

14. This Court has personal jurisdiction over Defendant because it is registered to conduct business in Oklahoma and has sufficient minimum contacts with Oklahoma.

15. Venue is likewise proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant conducts much of its business in this District and Defendant has caused harm to Class Members residing in this District.

FACTUAL ALLEGATIONS

A. OK Foods collects and stores thousands of current and former employees' PII and failed to provide adequate data security to protect it.

16. OK Foods, which is headquartered in Arkansas with locations in Oklahoma, was founded more than eighty (80) years ago and has evolved from a livestock and poultry feed manufacturer to one of the world's largest fully integrated chicken producers.

17. Currently OK Foods, a publicly traded company, employs over three thousand five hundred (3,500) employees, has tens of thousands of former employees, and is a major player in its industry. In addition to operating hatcheries, farms, feed mills, and processing plants across the country, OK Foods prides itself on "nourishing [its] consumers, [its] employees, our environment, and [its] shareholders."[4] OK Foods also touts on its website its company values of honesty, responsibility, respect, service, and justice.[5]

[4] https://www.okfoods.com/about-us/ (last accessed June 1, 2021).
[5] *Id.*

18. OK Foods claims it "understands the importance of protecting the security of [] Personal Info."[6] Moreover, OK Foods promises that "all Personal Info is encrypted and stored on secured servers."

B. OK Foods' inadequate data security exposed its current and former employees' sensitive PII.

19. Between April 22, 2020 and April 30, 2020, an unknown third party gained access to an OK Foods' employee's email account where highly sensitive employee data was being contained, unencrypted.

20. Between April 22, 2020 and April 30, 2020, unauthorized, unknown third party cyber criminals accessed OK Foods' employees' PII, which included names and Social Security numbers.

21. This incident is referred to herein as the "Data Breach."

22. Plaintiffs received data breach notice letters from OK Foods, both dated April 15, 2021 (collectively, the "Notice Letter"). Plaintiff Johnson's Notice Letter is attached hereto as **Exhibit 1** and Plaintiff Coffey's Notice Letter is attached hereto as **Exhibit 2**.

23. The Notice Letter was sent to Plaintiffs and the Class almost a full year after the Data breach occurred and includes the following:

> **What Happened?**
>
> As a result of a phishing incident, an unauthorized party obtained access to an OK Foods employee's email account.

[6] https://www.okfoods.com/privacy-policy (last accessed June 1, 2021).

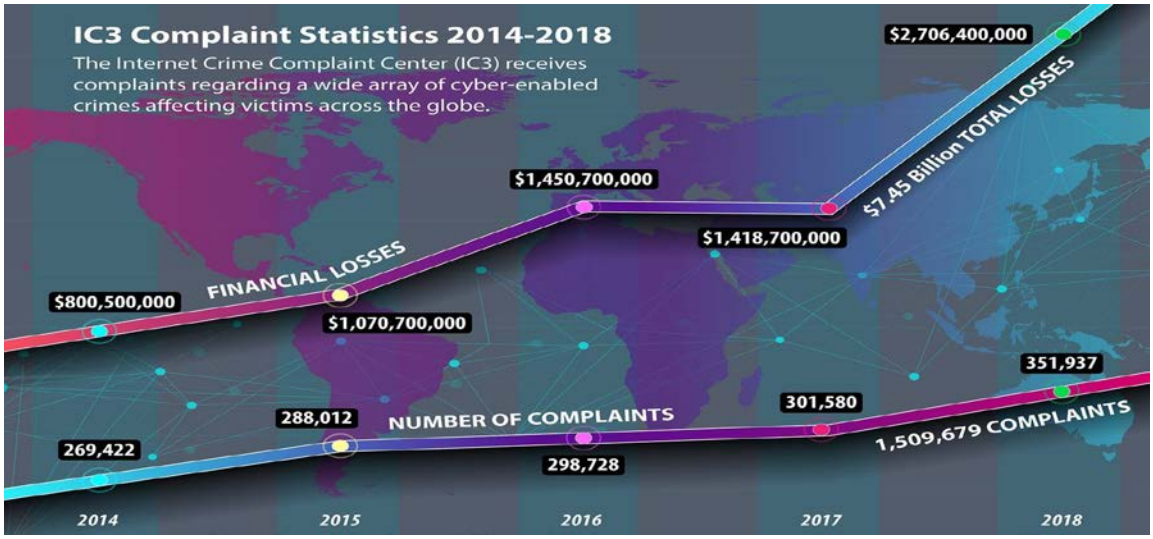
> **What Are We Doing?**
>
> Upon learning of the issue, we secured the account and commenced a prompt and thorough investigation. As part of our investigation, we have worked very closely with external cybersecurity professionals. After an extensive forensic investigation and manual email review, we determined on March 18, 2021 that the impacted email account, which was accessed between April 22, 2020 and April 30, 2020, contained some of your personal information. We have no evidence that your information has been misused. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.
>
> **What Information Was Involved?**
>
> The email account that was accessed contained some of your personal information, specifically your full name and Social Security number.

24. After receiving the Notice Letter, it is reasonable for recipients, including Plaintiffs and Class Members, to believe that the risk of future harm (including identity theft) is substantial and imminent, and to take steps to mitigate that substantial risk of future harm. In fact, in OK Foods' letter, it warns affected individuals of the "potential misuse of your information," and that impacted individuals should, among other things, "remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis." *See* **Exhibit 1** and **Exhibit 2**.

C. The PII exposed by OK Foods as a result of its inadequate data security is highly valuable on the black market.

25. The information exposed by OK Foods is a virtual goldmine for phishers, hackers, identity thieves and cyber criminals.

26. This exposure is tremendously problematic. Cybercrime is rising at an alarming rate, as shown in the FBI's Internet Crime Complaint statistics chart shown below:



27. By 2013, it was being reported that nearly one out of four data breach notification recipients becomes a victim of identity fraud.[7]

28. Stolen PII is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

29. When malicious actors infiltrate companies and copy and exfiltrate the PII that those companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[8]

---

[7] Pascual, Al, "2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters," *Javelin* (Feb. 20, 2013).

[8] *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce, Dec. 28, 2020, *available at:* https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last accessed July 28, 2021).

30. For example, when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to show, PII about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[9]

31. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200[10]. Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web[11]. Criminals can also purchase access to entire company data breaches from $900 to $4,500[12].

---

[9] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, *available at:* https://www.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last accessed July 28, 2021).

[10] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 28, 2021).

[11] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed July 28, 2021).

[12] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed July

32. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems[13].

33. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

34. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[14]

28, 2021).

[13] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 28, 2021).

[14] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*,

35. Because of this, the information compromised in the Data Breach here is significantly more harmful to lose than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

36. The PII compromised in the Data Breach demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[15]

37. Once PII is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the victim, as well as PII from family, friends and colleagues of the original victim.

38. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.

NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited July 28, 2021).

[15] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited July 28, 2021).

39. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiffs and Class Members that their PII had been stolen. It took Defendant over a year to determine the information had been compromised and notify Plaintiffs of the compromise.

40. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

41. Data breaches facilitate identity theft as hackers obtain consumers' PII and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

42. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PII to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[16] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage

[16] *See* Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited July 28, 2021).

to their credit records . . . [and their] good name."[17]

D. OK Foods Failed to Comply with Federal Trade Commission Requirements.

43. Federal and State governments have established security standards and issued recommendations to minimize data breaches and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[18]

44. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[19] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the

[17] *Id.*
[18] *See* Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited July 28, 2021).
[19] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited July 28, 2021).

event of a breach.[20]

45. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[21]

46. Highlighting the importance of protecting against phishing and other types of data breaches, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PII, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[22]

47. By negligently securing Plaintiffs' and Class Members' PII and allowing an unknown third-party cybercriminal to access an OK Foods employee's email account in order to access unencrypted employees' PII, OK Foods failed to employ reasonable and appropriate measures to protect against unauthorized access to confidential employee data. OK Foods' data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

---

[20] *Id.*
[21] Federal Trade Commission, *Start With Security*, *supra footnote 17*.
[22] Federal Trade Commission, *Privacy and Security Enforcement Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited July 28, 2021).

E. Plaintiff Johnson's Experience

48. Plaintiff Johnson was employed by OK Foods in or around September 2016 in Muldrow, Oklahoma.

49. On or around April 15, 2021, Plaintiff Johnson received the Notice Letter from OK Foods informing him of the Data Breach.

50. After receiving notification of the Data Breach, Plaintiff Johnson noticed a dramatic uptick in the amount and frequency of phishing emails he was receiving.

51. As a direct and traceable result of the Data Breach, Plaintiff Johnson has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on the telephone and sorting through his unsolicited emails, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This is time that has been lost forever and cannot be recaptured.

52. Plaintiff Johnson is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

53. Plaintiff Johnson stores all documents containing his PII in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for the few online accounts that he has.

54. Plaintiff Johnson has suffered actual, concrete injury in the form of damages to, and diminution in, the value of his PII – a form of intangible property that Plaintiff Johnson entrusted to Defendant for the purpose of his employment. This PII was compromised in, and has been diminished as a result of, the Data Breach.

55. Plaintiff Johnson has also suffered actual, concrete injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a direct and traceable result of the Data Breach, and has stress, anxiety and increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft which he now faces.

56. Plaintiff Johnson has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII resulting from the compromise of his PII, especially his Social Security number, in combination with his full name, which PII is now in the hands of cyber criminals and other unauthorized third parties.

57. Knowing that thieves stole his PII, including his Social Security Number and potentially his driver's license number and other PII that he was required to provide to OK Foods, and knowing that his PII will be sold on the dark web, has caused Plaintiff Johnson great anxiety.

58. Additionally, Plaintiff Johnson has not been involved in any data breaches and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. He deletes any and all electronic documents containing his PII and destroys any documents that may contain any of his PII, or that may contain any information that could otherwise be used to compromise his PII.

59. Plaintiff Johnson has a continuing interest in ensuring that his PII which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches.

60. As a direct and traceable result of the Data Breach, Plaintiff Johnson will continue to be at heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come and will have to pay an identity monitoring company for the rest of his life to protect his exposed PII.

F. Plaintiff Coffey's Experience

61. Plaintiff Coffey was employed by OK Foods in or around April 2016 in Fort Smith, Arkansas for one day.

62. On or around April 15, 2021, Plaintiff Coffey received the Notice Letter from OK Foods informing her of the Data Breach.

63. Beginning shortly after the verified Data Breach period and continuing now for over a year, Ms. Coffey has been notified through the Experian credit bureau of numerous "hard inquiries"[23] that she did not initiate.

64. As a result of the Data Breach, Plaintiff Coffey has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, including but not limited to, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts with much more frequency than she had done in the past. This is time that has been lost forever and cannot be recaptured.

[23] A "hard inquiry" or a "hard pull" occurs when you apply for a new line of credit, such as a credit card or loan. It means that a creditor has requested to look at your credit file to determine how much risk you pose as a borrower. Hard inquiries show up on your credit report and can negatively impact your credit score. *See* https://www.experian.com/blogs/ask-experian/what-is-a-hard-inquiry/ (last accessed July 27, 2021).

65. Plaintiff Coffey's PII has never been involved in any other prior data breaches and she is very careful about sharing her PII. In fact, Plaintiff Coffey has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

66. Plaintiff Coffey stores all documents containing her PII in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for the few online account that she has.

67. Plaintiff Coffey has suffered actual, concrete injury in the form of damages to, and diminution in, the value of her PII – a form of intangible property that Plaintiff Coffey entrusted to Defendant for the purpose of her employment. This PII was compromised in the Data Breach and, as a direct result thereof, its value has diminished.

68. Plaintiff Coffey has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has stress and anxiety accompanied by daily increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

69. Plaintiff Coffey has suffered present and increased risk arising from the substantially increased risk of fraud, identity theft, and misuse of her PII resulting from the compromise of her PII, especially her Social Security number, in combination with her full name, which PII is now in the hands of cyber criminals and other unauthorized third parties and has already been fraudulently used.

70. Knowing that thieves stole and now possess her PII, including her Social Security number and potentially other PII that she was required to provide to OK Foods,

and knowing that her PII will be sold on the dark web, has caused Plaintiff Coffey great stress and anxiety.

71. Plaintiff Coffey has a continuing interest in ensuring that her PII which, upon information and belief, remains in the possession and control of Defendant, is protected and safeguarded from future data breaches.

72. As a direct and traceable result of the Data Breach, Plaintiff Coffey will, for years to come, be at an imminent risk of financial fraud, identity theft, other forms of cybercrimes, and the attendant damages and will have to pay for credit and identity theft monitoring for the rest of her life in order to protect her exposed PII.

G. Plaintiffs and the Class Members suffered damages.

73. The ramifications of Defendant's failure to keep current and former employees' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.[24]

74. The PII belonging to Plaintiffs and Class Members is private, sensitive in nature, and was left inadequately protected by Defendant who did not obtain Plaintiffs' or Class Members' consent to disclose such PII to any other person as required by applicable law and industry standards.

75. Defendant required Plaintiffs and Class Members to provide their PII, including full names and Social Security numbers. Implied in these exchanges was a

[24] *2014 LexisNexis True Cost of Fraud Study, available at:* https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed July 28, 2021).

promise by Defendant to ensure that the PII of Plaintiffs and Class Members in its possession was only used to provide the agreed-upon compensation and other employment benefits from Defendant.

76. Plaintiffs and Class Members, therefore, did not receive the benefit of the bargain with Defendant, because providing their PII to Defendant was in exchange for Defendant's implied agreement to secure it and keep it safe.

77. The Data Breach was a direct and proximate result of OK Foods' failure to: (a) properly safeguard and protect Plaintiffs' and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' PII; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

78. Defendant had the resources necessary to prevent the Data Breach, but neglected to implement adequate data security measures, despite its obligations to protect current and former employees' PII, and despite its public statements that OK Foods "understands the importance of protecting the security of [] Personal Info" and OK Foods' promise that "all Personal Info is encrypted and stored on secured servers."

79. Had Defendant remedied the deficiencies in its data security training and protocols, and adopted security measures recommended by experts in the field, it would have prevented the intrusion leading to the theft of PII.

80. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

81. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[25]

82. As a direct result of the Defendant's failures to prevent the Data Breach, Plaintiffs and Class Members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft, and/or unauthorized use of their PII;

b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts

[25] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last accessed July 28, 2021).

spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

d. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII in its possession; and

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

83. In addition to a remedy for the economic harm, Plaintiffs and Class Members maintain an undeniable interest in ensuring that their PII is secure, remains secure, and is not subject to further misappropriation and theft.

84. To date, other than providing a woefully inadequate twelve (12) months of credit monitoring and identity protection services, Defendant does not appear to be taking any measures to assist Plaintiffs and Class Members other than simply telling them to review their financial records and credit reports on a regular basis.

85. This type of recommendation, however, does not require Defendant to expend any effort to protect Plaintiffs' and Class Members' PII.

86. Defendant's failure to adequately protect Plaintiffs' and Class Members' PII has resulted in Plaintiffs and Class Members having to undertake tasks requiring extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money – while Defendant sits by and does nothing to assist those affected by the Data Breach. Instead, as Defendant's Notice Letter indicates, it is putting the burden on Plaintiffs

and Class Members to discover possible fraudulent activity and identity theft.

87. Defendant's offer of 12 months of identity monitoring and identity protection services to Plaintiffs and Class Members is woefully inadequate. While some harm has begun already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is acquired and when it is used. Furthermore, identity theft monitoring services only alert someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's PII) – they do not prevent identity theft.[26] This is especially true for many kinds of medical identity theft, for which most credit monitoring plans provide little or no monitoring or protection. Although their PII was improperly exposed in or about April 2020, affected current and former employees were not notified of the Data Breach until a year later, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach. As a result of OK Foods' delay in detecting and notifying current and former employees of the Data Breach, the risk of fraud for Plaintiffs and Class Members has been driven even higher.

CLASS ACTION ALLEGATIONS

87. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this action on behalf of themselves and the following proposed Nationwide Class, defined as follows:

[26] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, Nov. 30, 2017, https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html (last visited July 28, 2021).

Nationwide Class

All persons residing in the United States who are current or former employees of OK Foods or any OK Foods affiliate, parent, or subsidiary, and had their PII compromised by an unknown third-party cybercriminal as a result of the Data Breach that occurred between April 22, 2020 and April 30, 2020.

In addition, Plaintiffs bring this action on behalf of the following proposed Oklahoma and Arkansas Subclasses defined as follows:

Oklahoma Subclass

All persons residing in the State of Oklahoma who are current or former employees of OK Foods or any OK Foods affiliate, parent, or subsidiary, and had their PII compromised as a result of the Data Breach that occurred between April 22, 2020 and April 30, 2020.

Arkansas Subclass

All persons residing in the State of Arkansas who are current or former employees of OK Foods or any OK Foods affiliate, parent, or subsidiary, and had their PII compromised as a result of the Data Breach that occurred between April 22, 2020 and April 30, 2020.

88. Both the proposed Nationwide Class and the proposed Oklahoma and Arkansas Subclasses will be collectively referred to as the Class, except where it is necessary to differentiate them.

89. Excluded from the proposed Class are any officer or director of Defendant; any officer or director of any affiliate, parent, or subsidiary of OK Foods; anyone employed by counsel in this action; and any judge to whom this case is assigned, his or her spouse, and members of the judge's staff.

90. **Numerosity.** Members of the proposed Class likely number in the tens of thousands and are thus too numerous to practically join in a single action. Membership in

the Class is readily ascertainable from Defendant's own records.

91. **Commonality and Predominance.** Common questions of law and fact exist as to all proposed Class Members and predominate over questions affecting only individual Class Members. These common questions include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant's inadequate data security measures were a cause of the Data Breach;

c. Whether Defendant owed a legal duty to Plaintiffs and the other Class Members to exercise due care in collecting, storing, and safeguarding their PII;

d. Whether Defendant negligently or recklessly breached legal duties owed to Plaintiffs and the Class Members to exercise due care in collecting, storing, and safeguarding their PII;

e. Whether Plaintiffs and the Class are at an increased risk for identity theft because of the Data Breach;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices for Plaintiffs' and Class Members' PII in violation Section 5 of the FTC Act;

g. Whether Plaintiffs and the other Class Members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

h. Whether Plaintiffs and the other Class Members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

92. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of the other Class Members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

93. **Typicality:** Plaintiffs' claims are typical of the claims of the Members of the Class. All Class Members were subject to the Data Breach and had their PII accessed by and/or disclosed to unauthorized third parties. Defendant's misconduct impacted all Class Members in the same manner.

94. **Adequacy of Representation:** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class Members they seek to represent; they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

95. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the other Class Members are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class Members to individually seek redress for Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized

litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

FIRST CAUSE OF ACTION
Negligence
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the Oklahoma and Arkansas Subclasses)

96. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

97. Defendant owed a duty to Plaintiffs and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members' PII from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, maintaining, and testing its data security systems to ensure that Plaintiffs' and Class Members' PII in Defendant's possession was adequately secured and protected.

98. Defendant owed a duty of care to Plaintiffs and Members of the Class to provide security, consistent with industry standards, to ensure that its protocols, systems, and networks adequately protected the PII of its current and former employees.

99. Defendant owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices. Defendant knew or should have known of the inherent risks in collecting and storing the PII of its current and former employees and exchanging it through email correspondence, and the

critical importance of adequately securing such information.

100. Plaintiffs and Class Members entrusted Defendant with their PII with the understanding that Defendant would safeguard it, that Defendant would not store it longer than necessary, and that Defendant was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

101. Defendant's own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their PII. Defendant's misconduct included failing to implement the necessary systems, policies, employee training and procedures necessary to prevent the Data Breach.

102. Defendant knew, or should have known, of the risks inherent in collecting and storing PII and the importance of adequate security. Defendant knew about – or should have been aware of – numerous, well-publicized data breaches affecting businesses in the United States.

103. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security to safeguard the PII of Plaintiffs and Class Members.

104. Plaintiffs' injuries and damages, as described below, are a reasonably certain consequence of OK Foods' breach of its duties.

105. Because Defendant knew that a breach of its systems would damage thousands of current and former OK Foods employees whose PII was inexplicably contained, unencrypted, in email accounts, Defendant had a duty to adequately protect its data systems and the PII contained therein.

106. Defendant had a special relationship with current and former employees, including with Plaintiffs and Class Members, by virtue of their being current or former employees. Plaintiffs and Class Members reasonably believed that Defendant would take adequate security precautions to protect their PII. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiffs' and Class Members' PII.

107. Through Defendant's acts and omissions, including Defendant's failure to provide adequate security and its failure to protect Plaintiffs' and Class Members' PII from being foreseeably accessed, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiffs and Class Members during the time it was within Defendant's possession or control.

108. In engaging in the negligent acts and omissions as alleged herein, which permitted an unknown third party to access an OK Foods' employee's email account containing the PII at issue, Defendant failed to meet the data security standards set forth under Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce." This prohibition includes failing to have adequate data security measures, which Defendant has failed to do as discussed herein.

109. Defendant's failure to meet this standard of data security established under Section 5 of the FTC Act is evidence of negligence.

110. Neither Plaintiffs nor the other Class Members contributed to the Data Breach as described in this Complaint.

111. As a direct and proximate cause of Defendant's actions and inactions,

including but not limited to its failure to properly encrypt its systems and otherwise implement and maintain reasonable security procedures and practices, Plaintiffs and Class Members have suffered and/or will suffer concrete injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PII is used; (ii) the publication and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports and password protection; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of employees and former employees in its continued possession; and (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the Oklahoma and Arkansas Subclasses)

112. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

113. Defendant offered employment to the current or former employees, including Plaintiffs and Class Members, in exchange for compensation and other employment benefits.

114. As a condition of employment, Defendant required Plaintiffs and Class Members to provide their PII, including names, addresses, dates of birth, Social Security numbers, driver's license numbers, and other personal information. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiffs and Class Members in its possession was only used to provide the agreed-upon compensation and other employment benefits from Defendant.

115. These exchanges constituted an agreement between the parties: Plaintiffs and Class Members would provide their PII in exchange for the prospect of employment and benefits provided by Defendant.

116. These agreements were made by Plaintiffs or Class Members who were employed by Defendant.

117. It is clear by these exchanges that the parties intended to enter into an agreement. Plaintiffs and Class Members would not have disclosed their PII to Defendant but for the prospect of Defendant's promise of compensation and other employment

benefits. Conversely, Defendant presumably would not have taken Plaintiffs' and Class Members' PII if it did not intend to provide Plaintiffs and Class Members compensation and other employment benefits.

118. Defendant was therefore required to reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure and/or use.

119. Plaintiffs and Class Members accepted Defendant's employment offer and fully performed their obligations under the implied contract with Defendant by providing their PII, directly or indirectly, to Defendant, among other obligations.

120. Plaintiffs and Class Members would not have provided and entrusted their PII to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their PII for uses other than compensation and other employment benefits from Defendant.

121. Defendant breached the implied contracts with Plaintiffs and Class Members by failing to reasonably safeguard and protect Plaintiffs' and Class Members' PII.

122. Defendant's failure to implement adequate measures to protect the PII of Plaintiffs and Class Members violated the purpose of the agreement between the parties: Plaintiffs' and Class Members' employment in exchange for compensation and benefits.

123. Defendant was on notice that its systems and data security protocols were inadequate yet failed to invest in the proper safeguarding of Plaintiffs' and Class Members' PII.

124. Instead of spending adequate financial resources to safeguard Plaintiffs' and Class Members' PII, which Plaintiffs and Class Members were required to provide to

Defendant, Defendant instead used that money for other purposes, thereby breaching its implied contracts it had with Plaintiffs and Class Members.

125. As a proximate and direct result of Defendant's breaches of its implied contracts with Plaintiffs and Class Members, Plaintiffs and the Class Members suffered damages as described in detail above.

THIRD CAUSE OF ACTION
Breach of Confidence
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the Oklahoma and Arkansas Subclasses)

126. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

127. At all times during Plaintiffs' and Class Members' interactions with Defendant as its employees, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' PII that Plaintiffs and Class Members provided to Defendant.

128. Plaintiffs' and Class Members' PII constitutes confidential and novel information. Indeed, Plaintiffs' and Class Members' Social Security numbers can be changed only with great difficulty and time spent, which still enables a threat actor to exploit that information during the interim; additionally, an individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

129. As alleged herein and above, Defendant's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

130. Plaintiffs and Class Members provided their respective PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized parties.

131. Defendant voluntarily received in confidence Plaintiffs' and Class Members' PII with the understanding that the PII would not be disclosed or disseminated to the public or any unauthorized third parties.

132. Due to Defendant's failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, not following best information security practices and by not providing proper employee training to secure Plaintiff's and Class Members' PII, Plaintiffs' and Class Members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

133. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and Class Members have suffered damages.

134. But for Defendant's disclosure of Plaintiffs' and Class Members' PII through its employee's email account, in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of

Plaintiffs' and Class Members' PII, as well as the resulting damages.

135. This disclosure of Plaintiffs' and Class Members' PII constituted a violation of Plaintiffs' and Class Members' understanding that Defendant would safeguard and protect the confidential and novel PII that Plaintiffs and Class Members were required to disclose to Defendant.

136. The concrete injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class Members' PII. Defendant knew its data security procedures for accepting and securing Plaintiffs' and Class Members' PII had numerous security and other vulnerabilities that placed Plaintiffs' and Class Members' PII in jeopardy.

137. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class Members have suffered and/or are at a substantial risk of suffering concrete injury that includes but is not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession; and (f) future costs in terms of time, effort, and money that will

be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

FOURTH CAUSE OF ACTION
Invasion of Privacy
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the Oklahoma and Arkansas Subclasses)

138. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

139. Oklahoma establishes the right to privacy in the Oklahoma Constitution's Right to Privacy clause. *See* Okla. Const. Art. II, Section 30.

140. Arkansas also establishes the right to privacy, as Arkansas courts have generally interpreted the common law right to privacy consistent with the four distinct privacy torts identified and defined in the Restatement (Second) of Torts.

141. Plaintiffs and Class Members had a legitimate and reasonable expectation of privacy with respect to their PII and were accordingly entitled to the protection of this personal information against disclosure to and acquisition by unauthorized third parties.

142. Defendant owed a duty to its employees, including Plaintiffs and Class Members, to keep their PII private and confidential.

143. The unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of PII, especially the PII that is the subject of this action, is highly offensive to a reasonable person.

144. This intrusion of privacy was an intrusion into a place or thing belonging to Plaintiffs and Class Members that was private and is entitled to remain private. Plaintiffs

and Class Members disclosed their PII to Defendant as part of their employment with Defendant but did so privately with the intention and understanding that the PII would be kept confidential and protected from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization. The Data Breach, which was caused by Defendant's negligent actions and inactions, constitutes an intentional interference with Plaintiffs' and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

145. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

146. Defendant invaded Plaintiff's and Class Members' privacy by failing to adequately implement data security measures, despite its obligations to protect current and former employees' highly sensitive PII.

147. Defendant's motives leading to the Data Breach were financially based. In order to save on operating costs, Defendant decided against the implement of adequate data security measures.

148. Defendant's intrusion upon Plaintiffs' and Class Members' privacy in order to save money constitutes an egregious breach of social norms.

149. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and Class Members.

150. As a proximate result of Defendant's acts and omissions, Plaintiffs' and Class Members' PII was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, obtained by, released to, stolen by, used by, and/or viewed by third parties without authorization, causing Plaintiffs and Class Members to suffer concrete damages as described herein.

151. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the PII maintained by Defendant can still be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized persons.

152. Plaintiffs and Class Members have no adequate remedy at law for the injuries they have suffered and are at imminent risk of suffering in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and Class Members.

FIFTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the Oklahoma and Arkansas Subclasses)

153. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

154. In light of their special relationship, Defendant became the guardian of Plaintiffs' and Class Members' PII. Defendant became a fiduciary, created by its undertaking and guardianship of its employees' PII, to act primarily for the benefit of those employees, including Plaintiffs and Class Members. This duty included the obligation to

safeguard Plaintiffs' and Class Members' PII and to timely detect and notify them in the event of a data breach.

155. In order to provide Plaintiffs and Class Members compensation and employment benefits, or to even consider Plaintiffs and Class Members for employment, Defendant required that Plaintiffs and Class Members provide their PII.

156. Defendant knowingly undertook the responsibility and duties related to the possession of Plaintiffs' and Class Members' PII for the benefit of Plaintiffs and Class Members in order to provide Plaintiffs and Class Members compensation and employment benefits.

157. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship with them. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to properly encrypt and otherwise protect Plaintiffs' and Class Members' PII. Defendant further breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely detect the Data Breach and notify and/or warn Plaintiffs and Class Members of the Data Breach.

158. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered or will suffer concrete injury, including but not limited to (a) actual identity theft; (b) the loss of the opportunity of how their PII is used; (c) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their PII; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (e) lost opportunity costs associated with efforts expended

and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII in its continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a direct and traceable result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

159. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

SIXTH CAUSE OF ACTION
Breach of Covenant of Good Faith and Fair Dealing
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the Oklahoma and Arkansas Subclasses)

160. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

161. As described above, when Plaintiffs and the Class Members provided their PII to Defendant, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties and industry standards to protect Plaintiffs' and Class Members' PII and to timely detect and notify them in the event of a data breach.

162. These exchanges constituted an agreement between the parties: Plaintiffs and Class Members were required to provide their PII in exchange for employment and benefits provided by Defendant.

163. It was clear by these exchanges that the parties intended to enter into an agreement. Plaintiffs and Class Members would not have disclosed their PII to Defendant but for the prospect of Defendant's promise of compensation and other employment benefits. Conversely, Defendant presumably would not have taken Plaintiffs' and Class Members' PII if it did not intend to provide Plaintiffs and Class Members compensation and other employment benefits.

164. Implied in these exchanges was a promise by Defendant to ensure that the PII of Plaintiffs and Class Members in its possession was only used to provide the agreed-upon compensation and other employment benefits from Defendant.

165. Plaintiffs and Class Members therefore did not receive the benefit of the bargain with Defendant, because they provided their PII in exchange for OK Foods' implied agreement to keep it safe and secure.

166. While Defendant had discretion in the specifics of how it met the applicable laws and industry standards, this discretion was governed by an implied covenant of good faith and fair dealing.

167. Defendant breached this implied covenant when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC and state statutes and regulations. These acts and omissions included: omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for Plaintiffs' and

Class Members' PII; storing the PII of former employees, despite any valid purpose for the storage thereof having ceased upon the termination of the employment relationship with those individuals; and failing to disclose to Plaintiffs and Class Members at the time they provided their PII to it that Defendant's data security systems, including training, auditing, and testing of employees, failed to meet applicable legal and industry standards.

168. Plaintiffs and Class Members did all or substantially all the significant things that the contract required them to do.

169. Likewise, all conditions required for Defendant's performance were met.

170. Defendant's acts and omissions unfairly interfered with Plaintiffs' and Class Members' rights to receive the full benefit of their contracts.

171. Plaintiffs and Class Members have been or will be harmed by Defendant's breach of this implied covenant in the many ways described above, including actual identity theft and/or imminent risk of certainly impending and devastating identity theft that exists now that cyber criminals have their PII, and the attendant long-term expense of attempting to mitigate and insure against these risks.

172. Defendant is liable for its breach of these implied covenants, whether or not it is found to have breached any specific express contractual term.

173. Plaintiffs and Class Members are entitled to damages, including compensatory damages and restitution, declaratory and injunctive relief, and attorney fees, costs, and expenses.

SEVENTH CAUSE OF ACTION
Declaratory and Injunctive Relief
(On behalf of Plaintiffs and Nationwide Class or, alternatively, the Oklahoma and Arkansas Subclasses)

174. Plaintiffs incorporate the foregoing paragraphs as though fully set forth herein.

175. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

176. As previously alleged, Plaintiffs and Class Members entered into an implied contract that required Defendant to provide adequate security for the PII it collected from Plaintiffs and Class Members.

177. Defendant owes a duty of care to Plaintiffs and Class Members requiring it to adequately secure their PII.

178. Defendant still possesses PII regarding Plaintiffs and Class Members.

179. Since the Data Breach, Defendant has announced few, if any, changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent future attacks.

180. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and Class Members. In fact, now that Defendant's insufficient data security is known to hackers, the PII in Defendant's possession is even more vulnerable to cyberattack.

181. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their PII and Defendant's failure to address the security failings that led to such exposure.

182. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

183. Plaintiffs, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant not transmit PII via unencrypted email;

f. Ordering that Defendant not store PII in email accounts;

g. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

h. Ordering that Defendant conduct regular computer system scanning and security checks;

i. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

j. Ordering Defendant to meaningfully educate its current, former, and prospective employees about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of themselves and all others similarly situated, respectfully request that the Court enter an order:

a. Certifying the proposed Class as requested herein;

b. Appointing Plaintiffs as Class Representatives and the undersigned counsel as Class Counsel;

c. Finding that Defendant engaged in the unlawful conduct as alleged herein;

d. Granting injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting OK Foods from engaging in the wrongful and unlawful acts described herein;

ii. requiring OK Foods to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring OK Foods to delete, destroy, and purge the PII of Plaintiffs and Class Members unless OK Foods can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring OK Foods to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members' PII;

v. prohibiting OK Foods from maintaining Plaintiffs' and Class Members' PII on a cloud-based database;

vi. requiring OK Foods to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on OK Foods' systems on a periodic basis, and ordering OK Foods to promptly correct any problems or issues detected by such third-party

security auditors;

vii. requiring OK Foods to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring OK Foods to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring OK Foods to segment data by, among other things, creating firewalls and access controls so that if one area of OK Foods' network is compromised, hackers cannot gain access to other portions of OK Foods' systems;

x. requiring OK Foods to conduct regular database scanning and securing checks;

xi. requiring OK Foods to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiffs and Class Members;

xii. requiring OK Foods to conduct internal training and education routinely and continually and, on an annual basis, inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring OK Foods to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the

preceding subparagraphs, as well as randomly and periodically testing employees' compliance with OK Foods' policies, programs, and systems for protecting PII;

xiv. requiring OK Foods to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor OK Foods' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring OK Foods to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring OK Foods to implement logging and monitoring programs sufficient to track traffic to and from OK Foods' servers;

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate OK Foods' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

xviii. requiring Defendant to design, maintain, and test its computer systems to ensure that PII in its possession is adequately secured and protected;

xix. requiring Defendant to detect and disclose any future data breaches in a timely and accurate manner;

xx. requiring Defendant to implement multi-factor authentication requirements, if not already implemented;

xxi. requiring Defendant's employees to change their passwords on a timely and regular basis, consistent with best practices; and

xxii. requiring Defendant to provide lifetime credit monitoring and identity theft repair services to Class Members.

e. Awarding Plaintiffs and Class Members damages;

f. Awarding Plaintiffs and Class Members pre-judgment and post-judgment interest on all amounts awarded;

g. Awarding Plaintiffs and the Class Members reasonable attorneys' fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the proposed Class, hereby demand a trial by jury as to all matters so triable.

Date: July 29, 2021

Respectfully Submitted,

*s/ William B. Federman*_____
William B. Federman, OBA #2853
Tyler J. Bean, OBA #33834
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
wbf@federmanlaw.com
tjb@federmanlaw.com

M. Anderson Berry*
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com

**Admitted pro hac vice*

Attorneys for Plaintiffs and the Class

CERTIFICATE OF SERVICE

I hereby certify that on July 29, 2021, a copy of the forgoing was served upon all counsel of record via ECF.

*s/ William B. Federman*_____